EXHIBIT 1

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

DECLARATION OF J. ALEX HALDERMAN
IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION

J. ALEX HALDERMAN declares, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. My name is J. Alex Halderman. I am a Professor of Computer Science and Engineering and the Director of the Center for Computer Security and Society at the University of Michigan in Ann Arbor, Michigan. I submit this Declaration in support of Plaintiffs Donna Curling, Donna Price, and Jeffrey Schoenberg (the "Curling Plaintiffs").

2. I have a Ph.D., a Master's Degree, and a Bachelor's Degree in Computer Science, all from Princeton University.

6. I have performed extensive hands-on security testing of the AccuVote TS and TSX electronic voting machines, which I understand are the two models of electronic voting machines used in Georgia. I published a peer-reviewed security evaluation of the AccuVote TS[1], and I performed a source code review of the AccuVote TSX as part of a study commissioned by the Secretary of State of California.[2] These studies discovered dozens of serious security vulnerabilities in the AccuVote hardware and software.

7. My curriculum vitae, including a list of honors and awards, research projects, and publications, is attached as Exhibit A.

Context: Cyberattacks, the 2016 Presidential Election, and Upcoming Elections

8. The 2016 presidential election was subject to unprecedented cyberattacks apparently intended to interfere with the election and undermine confidence in the voting process. For example, attackers broke into the email system of the Democratic National Committee and, separately, into the email account of John Podesta, the chairman of Secretary Clinton's campaign. Exhibits

---

[1] Ariel J. Feldman, J. Alex Halderman & Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*, Princeton University (2006), http://usenix.org/events/evt07/tech/full_papers/feldman/feldman.pdf.

[2] Joseph A. Calandrino et al., *Source Code Review of the Diebold Voting System*, University of California, Berkeley (2007), http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-source-public-jul29.pdf.

B and C. The attackers leaked private messages from both hacks. Attackers also attempted to breach election-related systems in at least 18 states, including Georgia. Exhibit D.[3] In at least two states, Illinois and Arizona, these attackers successfully infiltrated the voter registration systems and stole voter data. Exhibit E. The U.S. Senate Select Committee on Intelligence has concluded that, in a small number of states, the attackers were in a position to alter or delete voter registration data.[4] Exhibit F. The Department of Homeland Security has stated that senior officials in the Russian government commissioned these attacks. Exhibit G.

9. Russia has sophisticated cyber-offensive capabilities, and it has shown a willingness to use them to hack elections elsewhere. For instance, according to published reports, during the 2014 presidential election in Ukraine, attackers linked to Russia sabotaged Ukraine's vote counting infrastructure, and Ukrainian officials succeeded only at the last minute in defusing vote-stealing malware that could

---

[3] Kim Zetter, *Was Georgia's Election System Hacked in 2016?*, POLITICO Magazine (July 18, 2018), https://www.politico.com/magazine/story/2018/07/18/mueller-indictments-georgia-voting-infrastructure-219018.

[4] Senate Intelligence Committee, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations*, at 1-2 (May 9, 2018), https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf.

have caused the wrong winner to be announced. Exhibit H. Countries other than Russia also have similarly sophisticated cyberwarfare capabilities.

10. In May 2018, the U.S. Senate Select Committee on Intelligence, charged with investigating cybersecurity threats to U.S. election infrastructure, reported its findings and recommendations.[5] The committee found serious vulnerabilities, including that "voting systems across the United States are outdated, and many do not have a paper record of votes as a backup counting system that can be reliably audited, should there be allegations of machine manipulation."[6] Moreover, "Paperless Direct Recording Electronic (DRE) voting machines"—the type used in Georgia—"are at highest risk for security flaws."[7]

11. Director of National Intelligence Dan Coats and Secretary of Homeland Security Kristjen Nielsen have warned as recently as August 2, 2018, that Russia is continuing to pursue its goal of interfering in our elections, including the upcoming midterm elections in November.[8]

12. Foreign governments could attempt to hack American voting machines to achieve a variety of goals, including undermining voter confidence

---

[5] *Id.*
[6] *Id.* at 4.
[7] *Id.*
[8] Brian Ries & Meg Wagner, White House press briefing, CNN (Aug. 2, 2018), https://www.cnn.com/politics/live-news/whpb-08-02-18/h_b4373e9f04f5da63237586ce450a0962.

and causing fraudulent outcomes. They could sabotage the machines to prevent them from functioning on Election Day, or to cause them to produce obviously incorrect results when votes are counted. They could also infiltrate the machines with malicious software in order to cause them to produce plausible but fraudulent results. I have written demonstration malicious software that executes these attacks against the models of electronic voting machines used in Georgia.

The Vulnerability of Georgia's Voting Machines to Cyberattack

13. More than 70% of American voters have their votes recorded on some form of paper, which provides permanent evidence of their intent in the event of a post-election audit or recount—33 states have a paper ballot, or at least a paper trail, for every vote. In Georgia, except for absentee voting, all ballots are cast on paperless[9] direct-recording electronic (DRE) computer voting machines that do not create a paper record of each vote. Georgia is one of only five states to use paperless machines statewide.[10]

---

[9] In election technology contexts, "paperless" refers to machines that lack a voter-verifiable paper record of each ballot. Although Georgia's machines print a paper summary of the election totals after polls close, they are still considered "paperless," since this summary tape does not provide a way for the voter to confirm that his or her vote has been properly recorded.

[10] Verified Voting, The Verifier – Polling Place Equipment – November 2018, https://www.verifiedvoting.org/verifier/ (last accessed Aug. 7, 2018).

14. Paperless DRE voting machines have been repeatedly shown to be vulnerable to cyberattacks that can change or erase votes, cast extra votes, or cause the machines to fail to operate on election day. Since paperless DREs do not generate a physical record of the vote, these attacks may be difficult or impossible to detect or to reverse. There is a broad scientific consensus that paperless DREs do not provide adequate security against cyberattacks.

15. To my knowledge, Georgia exclusively uses Premier/Diebold (Dominion) AccuVote TS and TSX voting machines. These particular models are probably the most well-studied by security researchers of any voting machines in the world. Over the past 15 years, I and other experts have repeatedly documented serious cybersecurity problems with these machines, in peer-reviewed and state-sponsored research studies. The vulnerabilities that affect Georgia's machines include numerous hardware and software security flaws, as well as architectural weaknesses that cannot be repaired through software updates. As a result, every DRE in use in Georgia is vulnerable to cyberattacks.

16. These voting machines are computers with reprogrammable software. An attacker who can modify that software by infecting the machines with malware can cause the machines to provide any result of the attacker's choosing. In tests, I have demonstrated that, in just a few seconds, anyone can install vote-stealing

malware on these voting machines that will silently alter all records of every vote.[11]

17. The first major study of these machines was carried out in 2003 by Kohno, Stubblefield, Rubin, and Wallach, who studied a leaked version of the source code and found many design errors and vulnerabilities.[12] Public concern in light of Kohno's study led the state of Maryland to authorize two security studies. The first, by SAIC, reported that the system was "at high risk of compromise."[13] The second, conducted by RABA, a security consulting firm, confirmed many of Kohno's findings and suggested design changes to the Diebold system.[14] A further security assessment was commissioned by the Ohio Secretary of State and carried

---

[11] A video documenting this result is publicly available. Hack247, *Princeton University Diebold Machine Hacking*, YouTube (Nov. 7, 2006), https://www.youtube.com/watch?v=2Vvq_YseZVc.

[12] Tadayoshi Kohno et al., *Analysis of an Electronic Voting System*, *in* IEEE Symposium on Security and Privacy, IEEE Computer Society Press (Feb. 27, 2004), http://avirubin.com/vote.pdf.

[13] Science Applications International Corporation, Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes, SAIC-6099-2003-261 (Sept. 2, 2003).

[14] RABA Technologies, *Trusted agent report: Diebold AccuVote-TS voting system*, (Jan. 20, 2004), http://euro.ecom.cmu.edu/program/courses/tcr17-803/TA_Report_AccuVote.pdf.

out by Compuware.[15] It examined several DRE systems, including the AccuVote TS, and identified a number of high-risk security problems.

18. In 2006, independent security researcher Harri Hursti examined the hardware and firmware of AccuVote TS and TSX systems. He discovered problems with a software update mechanism that could allow malicious parties to infect the machines with malicious code.[16] Also in 2006, I and collaborators at Princeton obtained an AccuVote TS from a private party and reverse engineered its hardware and software.[17] Our study confirmed the results of the earlier security reviews and discovered a variety of additional serious vulnerabilities.

19. We demonstrated the vulnerabilities of the AccuVote TS by developing a piece of malware (malicious software) that could infect the machines and steal votes. The malware modifies all of the vote records, audit logs, and protective counters stored by the machine, so that even careful forensic examination of the files would find nothing amiss. The malware was programmed to inspect each ballot as it was cast and modify the minimum number of votes

---

[15] Compuware Corp., *Direct recording electronic (DRE) Technical Security Assessment Report* (Nov. 21, 2003), http://www.sos.state.oh.us/sos/hava/compuware112103.pdf.
[16] Harri Hursti, *Diebold TSx Evaluation Security Alert: May 11, 2006 Critical Security Issues with Diebold TSx*, IssueLab (May 11, 2006), https://www.issuelab.org/resources/1294/1294.pdf.
[17] Feldman, *supra* note 1.

necessary to ensure that the attacker's favored candidate always had at least a certain percentage of the vote total.

20. We also developed a voting machine virus that could spread the vote-stealing malware automatically and silently from machine to machine during normal pre- and post-election activities. The virus propagated via the removable memory cards that election officials use to program the ballot design before every election and to offload election results. By exploiting vulnerabilities in the AccuVote software, an infected memory card can spread the voting machine virus to the machine.

21. Once installed, the virus copies itself to every memory card inserted into the infected machine. If those cards were inserted into other machines, they too would become infected. As a result, an attacker could infect a large population of machines while only having temporary physical access to a single machine or memory card.

22. In 2007, the Secretary of State of California organized a comprehensive election security examination, the California Top-to-Bottom Review (TTBR[18]), which examined systems including the AccuVote TSX. I was part of a team of six experts who spent approximately 30 days examining the

[18] Cal. Sec'y of State, *Top-to-Bottom Review*, http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/ (last accessed Aug. 7, 2018).

Georgia Should Replace DREs With Paper Ballots and Appropriate Post-Election Audits

57. All of Georgia's votes (that are not cast via absentee ballot) are recorded on DRE voting machines that do not generate any paper record of the individual votes. The only practical way to safeguard Georgia's upcoming election is to discontinue the use of Georgia's DREs, require the use of optical scan paper ballots throughout Georgia, and mandate auditing of the results to ensure that the optical scanners were not attacked with malware to infect the automated counting of the ballots.

Dated: August 7, 2018
Ann Arbor, Michigan

J. ALEX HALDERMAN

EXHIBIT B

APRIL GLASER SECURITY 07.27.16 9:30 AM

HERE'S WHAT WE KNOW ABOUT RUSSIA AND THE DNC HACK

GETTY IMAGES

AS THE DEMOCRATIC National Convention continues its week-long stay in Philadelphia, accusations of Russian hacking continue to cloud the proceedings. At this point, it seems likely that Russia is responsible. What's less clear is what that will mean going forward.

It's been a bad stretch for the Democratic National Committee. Hackers broke into its servers months ago, stealing private emails, opposition research, and campaign correspondence. Last Friday, Wikileaks made nearly 20,000 of those private emails public, revealing embarrassing details of the political machine's inner workings. DNC official allege that the Russian government is behind the breach. The *New York Times* reports that US intelligence agencies increasingly share that opinion. According to a number of top cybersecurity researchers, they're probably right.

A Brief History of a Hack

News of the hack of the Democratic National Committee first broke in mid-June. That's when Crowdstrike, a firm that analyzes threats to network security, revealed that the DNC had called it in to inspect the party's servers, where it found "two separate Russian intelligence-affiliated adversaries present in the DNC network." Crowdstrike released a comprehensive report of its findings on June 14, which accompanied a *Washington Post* article detailing the attacks. One of the hacking groups, Crowdstrike found, had access to the DNC servers for almost a year.

A day after that report, someone calling themselves Guccifer 2.0 (an allusion to notorious hacker Guccifer) claimed responsibility for the hack in a blog post. Through the blog and an accompanying Twitter account, Guccifer 2.0 refuted Crowdstrike's claims that this was a Russian operation, instead calling himself a "lone hacker." He also claimed to have handed much of the DNC bounty to Wikileaks.

The following week, two cybersecurity firms, Fidelis Cybersecurity and Mandiant, independently corroborated Crowdstrike's assessment that Russian hackers infiltrated DNC networks, having found that the two groups that hacked into the DNC used malware and methods identical to those used in other attacks attributed to the same Russian hacking groups.

But some of the most compelling evidence linking the DNC breach to Russia was found at the beginning of July by Thomas Rid, a professor at King's College in London, who discovered an identical command-and-control address hardcoded into the DNC malware that was also found on malware used to hack the German Parliament in 2015. According to German security officials, the malware originated from Russian military intelligence. An identical SSL certificate was also found in both breaches.

The evidence mounts from there. Traces of metadata in the document dump reveal various indications that they were translated into Cyrillic. Furthermore, while Guccifer 2.0 claimed to be from Romania, he was unable to chat with Motherboard journalists in coherent Romanian. Besides which, this sort of hacking wouldn't exactly be outside of Russian norms.

"It doesn't strain credulity to look to the Russians," says Morgan Marquis-Boire, a malware expert with CitizenLab. "This is not the first time that Russian hackers has been behind intrusions in US government, and it seems unlikely that it will be the last." Last year Russian hackers were able to breach White House and State

Department email servers, gleaning information even from President Obama's Blackberry.

Meanwhile, the Kremlin has denied Russian involvement in the DNC breach. But the reverberations continue; DNC Chairwoman Debbie Wasserman Schultz will resign at the end of the week, after emails revealed what many view as the unfair treatment of Bernie Sanders.

From Russia With Love

As compelling as the evidence is, there's still a small amount of room to argue that Guccifer 2.0 was a lone actor, an individual motivated by hacktivist ideals of dismantling state power. He wouldn't be the first. And in a recent interview on NBC, Julian Assange of Wikileaks gave a soft disavowal of claims that his whistleblowing organization is in cahoots with Russian intelligence, "Well, there is no proof of that whatsoever," he said. "We have not disclosed our source, and of course, this is a diversion that's being pushed by the Hillary Clinton campaign."

This is, of course, the same Assange who boasts responsibility for helping find Snowden a home in Russia and Wikileaks publicly criticized the Panama Papers for implicating Putin in financial misdeeds. He's also an outspoken frequent critic of Hillary Clinton's time at the State Department. A damning document dump the weekend before Clinton's nomination arguably aligns with both Russian interests and his own.

If the allegations do prove correct, this is an unprecedented step for Russia. Hacking is nothing new, but publicizing documents to attempt to sway an election certainly is. Putin would clearly prefer a Trump presidency. The billionaire Republican candidate is a longtime admirer of Putin's, and has publicly stated that he wouldn't necessarily defend NATO allies against a Russian invasion. To top it all off, Trump's campaign manager, Paul Manafort, formerly worked as an advisor to Viktor Yanukovych, the Russian-backed President of Ukraine before he was ousted in 2014.

"Due to the nature and timing of this hack, it all seems very political," says Marquis-Boire.

And there's a whole lot of election left—and likely more leaks to come with it. On Sunday, a Twitter user asked Wikileaks if more DNC leaks were on their way. The reply: "We have more coming."

Update: In a press conference Wednesday, Republican presidential candidate Donald Trump invited Russia to retrieve "missing" emails from Hillary Clinton's campaign and release them. Cybersecurity experts described the remarks as "unprecedented" and "possibly illegal."

EXHIBIT C

The New York Times | http://nyti.ms/2eqNSVY

Private Security Group Says Russia Was Behind John Podesta's Email Hack

By NICOLE PERLROTH and MICHAEL D. SHEAR OCT. 20, 2016

SAN FRANCISCO — At the start of 2014, President Obama assigned his trusted counselor, John D. Podesta, to lead a review of the digital revolution, its potential and its perils. When Mr. Podesta presented his findings five months later, he called the internet's onslaught of big data "a historic driver of progress." But two short years later, as chairman of Hillary Clinton's presidential campaign, Mr. Podesta would also become one of the internet's most notable victims.

On Thursday, private security researchers said they had concluded that Mr. Podesta was hacked by Russia's foreign intelligence service, the GRU, after it tricked him into clicking on a fake Google login page last March, inadvertently handing over his digital credentials.

For months, the hackers mined Mr. Podesta's inbox for his most sensitive and potentially embarrassing correspondence, much of which has been posted on the WikiLeaks website. Additions to the collection on Thursday included three short

email exchanges between Mr. Podesta and Mr. Obama himself in the days leading up to his election in 2008.

Mr. Podesta's emails were first published by WikiLeaks earlier this month. The release came just days after James R. Clapper Jr., the director of national intelligence, and the Department of Homeland Security publicly blamed Russian officials for cyberattacks on the Democratic National Committee, in what they described as an effort to influence the American presidential election.

To date, no government officials have offered evidence that the same Russian hackers behind the D.N.C. cyberattacks were also behind the hack of Mr. Podesta's emails, but an investigation by the private security researchers determined that they were the same.

Threat researchers at Dell SecureWorks, an Atlanta-based security firm, had been tracking the Russian intelligence group for more than a year. In June, they reported that they had uncovered a critical tool in the Russian spy campaign. SecureWorks researchers found that the Russian hackers were using a popular link shortening service, called Bitly, to shorten malicious links they used to send targets fake Google login pages to bait them into submitting their email credentials.

The hackers made a critical error by leaving some of their Bitly accounts public, making it possible for SecureWorks to trace 9,000 of their links to nearly 4,000 Gmail accounts targeted between October 2015 and May 2016 with fake Google login pages and security alerts designed to trick users into turning over their passwords.

Among the list of targets were more than 100 email addresses associated with Hillary Clinton's presidential campaign, including Mr. Podesta's. By June, 20 staff members for the campaign had clicked on the short links sent by Russian spies. In June, SecureWorks disclosed that among those whose email accounts had been targeted were staff members who advised Mrs. Clinton on policy and managed her travel, communications and campaign finances.

Two security researchers who have been tracking the GRU's spearphishing campaign confirmed Thursday that Mr. Podesta was among those who had inadvertently turned over his Google email password. The fact that Mr. Podesta was among those breached by the GRU was first disclosed Thursday by Esquire and the Motherboard blog, which published the link Russian spies used against Mr. Podesta.

"The new public data confirming the Russians are behind the hack of John Podesta's email is a big deal," Jake Sullivan, Mrs. Clinton's senior policy adviser, said Thursday. "There is no longer any doubt that Putin is trying to help Donald Trump by weaponizing WikiLeaks."

The new release of Mr. Podesta's email exchange with Mr. Obama from 2008 made clear that Mr. Obama's team was confident he would win.

In one of the emails, Mr. Podesta wrote Mr. Obama a lengthy memo in the evening on Election Day recommending that he not accept an invitation from President George W. Bush to attend an emergency meeting of the Group of 20 leaders.

"Attendance alongside President Bush will create an extremely awkward situation," the memo said. "If you attempt to dissociate yourself from his positions, you will be subject to criticism for projecting a divided United States to the rest of the world. But if you adopt a more reserved posture, you will be associated not only with his policies, but also with his very tenuous global standing."

The White House did not respond to questions about the email.

Correction: October 22, 2016

An article on Friday about suspected email hacking by Russia's foreign intelligence service misstated the name of one organization that first disclosed that a presidential counselor, John D. Podesta, was among those whose accounts were breached. The blog is Motherboard, not VICE Motherload.

Nicole Perlroth reported from San Francisco, and Michael D. Shear from Washington.

Follow The New York Times's politics and Washington coverage on Facebook and Twitter, and sign up for the First Draft politics newsletter.

A version of this article appears in print on October 21, 2016, on page A14 of the New York edition with the headline: Private Security Group Says Russia Was Behind Hack of Clinton Campaign Chairman.

EXHIBIT D

NEWS AUG 30 2016, 4:54 AM ET

Russians Hacked Two U.S. Voter Databases, Officials Say

by ROBERT WINDREM, WILLIAM M. ARKIN and KEN DILANIAN

Hackers based in Russia were behind two recent attempts to breach state voter registration databases, fueling concerns the Russian government may be trying to interfere in the U.S. presidential election, U.S. intelligence officials tell NBC News.

The breaches included the theft of data from as many as 200,000 voter records in Illinois, officials say.

The incidents led the FBI to send a "flash alert" earlier this month to election officials nationwide, asking them to be on the lookout for any similar cyber intrusions.

One official tells NBC News that the attacks have been attributed to Russian intelligence agencies.

"This is the closest we've come to tying a recent hack to the Russian government," the official said.

That person added that "there is serious concern" that the Kremlin may be seeking to sow uncertainty in the U.S. presidential election process.

Voters cast their ballots at ChiArts High School on March 15 in Chicago, Illinois. Scott Olson / Getty Images

Two other officials said that U.S. intelligence agencies have not yet concluded that the Russian government is trying to do that, but they are worried about it.

They said the Russians have long conducted cyber espionage on political targets. The question now is whether they are moving into a covert intelligence operation designed to destabilize the U.S. political process.

The alert, first reported by Yahoo News, provided IP addresses associated with the hack attempts, though it did not mention Russia.

One of the IP addresses was involved in both breaches, the FBI alert said.

"The FBI is requesting that states contact their Board of Elections and determine if any similar activity to their logs, both inbound and outbound, has been detected," the alert said.

The bulletin does not identify the targeted states, but officials told NBC News they were Illinois and Arizona. Illinois officials said in July that they shut down their state's voter registration after a hack. State officials said Monday the hackers downloaded information on as many 200,000 people.

State officials told the Chicago Tribune they were confident no voter record had been deleted or altered.

In Arizona, officials said, hackers tried to get in using malicious software but were unsuccessful. The state took its online voter registration down for nine days, beginning in late June, after malware was discovered on a county election official's computer. But the state concluded that the system was not successfully breached.

Those incidents led Homeland Security Secretary Jeh Johnson to host a call earlier this month with state election officials to talk about cybersecurity and election infrastructure.

Johnson said DHS isn't aware of any specific cyber threat against election-related networks, but he urged officials to examine how to better secure their systems, according to a summary of the call put out by the department.

U.S. intelligence officials have previously said Russian intelligence agencies were behind hacks into the Democratic National Committee and related organizations. There has been a long running debate among intelligence analysts about what Russia is up to.

Voting systems have not been considered "critical infrastructure," by the Department of Homeland Security, so they are not subject to federal government protections.

Independent assessments have found that many state and local voting system are extremely vulnerable to hacking.

ROBERT WINDREM

WILLIAM M. ARKIN

KEN DILANIAN

TOPICS U.S. NEWS, INVESTIGATIONS, SECURITY, WORLD

FIRST PUBLISHED AUG 29 2016, 6:05 PM ET

NEXT STORY Trump's Victory Has Fearful Minorities Buying Up Guns

EXHIBIT E

U.S. official: Hackers targeted voter registration systems of 20 states

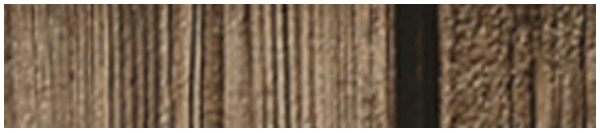
In this June 5, 2015, file photo, the Homeland Security Department headquarters in northwest Washington. A Homeland Security Department official says hackers have targeted the voter registration systems of more than 20 states in recent months. FBI Director James Comey told lawmakers this week that the agency is looking "very, very hard" at Russian hackers who may try to disrupt the U.S. election. (Susan Walsh / AP)

By Tribune news services

SEPTEMBER 30, 2016, 4:42 PM | WASHINGTON

Hackers have targeted the voter registration systems of more than 20 states in recent months, a Homeland Security Department official said Friday.

The disclosure comes amid heightened concerns that foreign hackers might undermine voter confidence in the integrity of U.S. elections. Federal officials and many cybersecurity experts have said it would be nearly impossible for hackers to alter an election's outcome because election systems are very decentralized and generally not connected to the internet.



The official who described detecting the hacker activity was not authorized to speak publicly on the subject and spoke to The Associated Press on condition of anonymity. It was unclear, the official said, whether the hackers were foreign or domestic, or what their motives might be. ABC News earlier reported that more than 20 states were targeted.

The FBI last month warned state officials of the need to improve their election security after hackers targeted systems in Illinois and Arizona. FBI Director James Comey told lawmakers this week that the agency is looking "very, very hard" at Russian hackers who may try to disrupt the U.S. election.

Last month, Donald Trump, the GOP nominee for president, suggested that he feared the general election "is going to be rigged."

The Homeland Security Department has stepped up its outreach to states and localities, but it is up to them to ask for help. So far, 19 states have expressed interest in a general "cyber hygiene" scan of key websites — akin to ensuring that windows in a home are properly closed, according to another Homeland Security official directly involved in securing local elections who also was not authorized to speak publicly about ongoing efforts.

The FBI has detected a variety of "scanning activities" that are early indications of hacking, Comey told the House Judiciary Committee this week.

The FBI held a conference call on Friday with the local officials who run elections in the battleground state of Florida. Meredith Beatrice, a spokeswoman for Secretary of State Ken Detzner, called it an "informational call related to elections security," but a person on the call who was not authorized to discuss it and requested anonymity said authorities had seen evidence of someone probing a local elections website.

Homeland Security Secretary Jeh Johnson spoke to state election officials by phone last month, encouraging them to implement existing technical recommendations to secure their election systems and ensure that electronic voting machines are not connected to the internet.

DHS is offering states more comprehensive, on-site risk and vulnerability checks. Only four states have expressed interest in the assessment, and because the election is only weeks away, the department will likely only be able to conduct an assessment of one state before Election Day on Nov. 8, the official said.

Two of the hacking attempts involved efforts to mine data from the Arizona and Illinois voter registration systems, according to Kay Stimson, a spokeswoman for the National Association of Secretaries of State. She said in Arizona a hacker tried to probe voter registration data, but never infiltrated the system, while in Illinois hackers got into the system, but didn't manipulate any data.

These systems have "nothing to do with vote casting or counting," Stimson said in an email. "While it is theoretically possible to disrupt an election by infiltrating a voter registration system, their compromise would not affect election results" and there are system controls in place to catch any fraud.

Rep. Henry Johnson, D-Ga., introduced two bills earlier this month that would require voting systems be designated as critical infrastructure and limit purchases of new voting systems that don't provide paper ballots, among other measures. It's unlikely the bills will be passed before the election.

The Homeland Security Department is already considering designating voting systems as critical infrastructure in the future, though it is unlikely to happen before the election, the second official said.

A presidential directive released in 2013 details 16 sectors that are considered critical infrastructure, including energy, financial services, healthcare, transportation, food and agriculture, and communications. The designation places responsibilities on the Homeland Security secretary to identify and prioritize those sectors, considering physical and cyber threats. The secretary is also required to conduct security checks and provide information about emerging and imminent threats.

Associated Press

This article is related to: Jeh Johnson, James Comey

EXHIBIT F

theguardian

Senators call for declassification of files on Russia's role in US election

Eight members of Senate intelligence committee hint that government may still hold secret information 'concerning the Russian government'

The eight senators did not directly accuse the Russian government or Donald Trump of wrongdoing. Photograph: Timothy A Clary/AFP/Getty Images

Spencer Ackerman in New York

Thursday 1 December 2016 11.07 EST

All of the Democratic and Democratic-aligned members of the Senate intelligence committee have hinted that significant information about Russian interference in the US presidential election remains secret and ought to be declassified.

The eight senators, including the incoming ranking member Mark Warner of Virginia, wrote to Barack Obama to request he declassify relevant intelligence on the election. They did not directly accuse the Russian government or President-elect Donald Trump, a Republican, of wrongdoing in the letter.

“We believe there is additional information concerning the Russian government and the US election that should be declassified and released to the public. We are conveying specifics through classified channels,” wrote Warner and his colleagues Ron Wyden of Oregon, Martin Heinrich of New Mexico, Mazie Hirono of Hawaii, Barbara Mikulski of Maryland and independent Angus King of Maine.

Jack Reed of Rhode Island, an honorary and non-voting member of the committee due to his seat as ranking member of the Senate armed services committee, also signed the letter, which was dated Tuesday and publicly released on Wednesday. No Republican joined the declassification call.

The outgoing ranking Democrat, Dianne Feinstein of California, signed the classified version of the letter sent to Obama.

Neither the terse letter nor discussions with sources on Capitol Hill detailed the particular intelligence concerning the Russians, its strength or its impact on the outcome of the election. Thus far, no credible evidence of vote fraud or electoral malfeasance exists, despite an evidence-free claim from Trump himself.

A spokesman for Wyden, Keith Chu, said the senator believed the intelligence needed to be declassified “immediately”, as it was in the “national interest that the American public should see it”.

It is understood this is the first declassification request by eight senators in at least twelve years.

On 7 October, the US director of national intelligence and the secretary of homeland security took the rare step of directly accusing Russia’s “senior-most” officials of ordering the breach of the Democratic National Committee’s digital networks. Director James Clapper and Secretary Jeh Johnson accused the Russians of attempting to “interfere” in the US election, something the Obama administration had previously suggested but did not allege publicly.

The FBI has acknowledged investigating such interference, but has reportedly not established any link to Trump or his campaign. Two US officials have told the Guardian that the FBI was reluctant to sign off on Clapper and Johnson’s public allegation.

Yet Harry Reid, the outgoing Democratic Senate leader, asserted without evidence in October that the FBI director, James Comey, “possess[es] explosive information about close ties and coordination between Donald Trump, his top advisers, and the Russian government”.

Unusually for any presidential nominee, and particularly for a Republican, Trump has exhibited a warmth toward the Russian president, Vladimir Putin, that has prompted a widespread expectation Trump will tilt US foreign policy toward Russia. Trump and Putin spoke soon after Trump’s electoral victory in a phone call heralded by the Kremlin.

There was no immediate comment from the White House or Clapper's office as to whether Obama would order the declassification or whether the intelligence agencies even support such a move.

Since you're here ...

... we have a small favour to ask. More people are reading the Guardian than ever but far fewer are paying for it. And advertising revenues across the media are falling fast. So you can see why we need to ask for your help. The Guardian's independent, investigative journalism takes a lot of time, money and hard work to produce. But we do it because we believe our perspective matters – because it might well be your perspective, too.

Fund our journalism and together we can keep the world informed.

Become a Supporter
Make a contribution
More news

Topics

US elections 2016 Russia US politics US Senate

Save for later Article saved
Reuse this content

EXHIBIT G

Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security

Release Date: October 7, 2016

For Immediate Release
DHS Press Office
Contact: 202-282-8010

The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts.

These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.

Some states have also recently seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company. However, we are not now in a position to attribute this activity to the Russian Government. The USIC and the Department of Homeland Security (DHS) assess that it would be extremely difficult for someone, including a nation-state actor, to alter actual ballot counts or election results by cyber attack or intrusion. This assessment is based on the decentralized nature of our election system in this country and the number of protections state and local election officials have in place. States ensure that voting machines are not connected to the Internet, and there are numerous checks and balances as well as extensive oversight at multiple levels built into our election process.

Nevertheless, DHS continues to urge state and local election officials to be vigilant and seek cybersecurity assistance from DHS. A number of states have already done so. DHS is providing several services to state and local election officials to assist in their cybersecurity. These services include cyber “hygiene” scans of Internet-facing systems, risk and vulnerability assessments, information sharing about cyber incidents, and best practices for securing voter registration databases and addressing potential cyber threats. DHS has convened an Election Infrastructure Cybersecurity Working Group with experts across all levels of government to raise awareness of cybersecurity risks potentially affecting election infrastructure and the elections process. Secretary Johnson and DHS officials are working directly with the National Association of Secretaries of State to offer assistance, share

information, and provide additional resources to state and local officials.

# # #

Last Published Date: October 7, 2016